

AT-S63 Version 2.0.0

Management Software for the

AT-9400 Series Layer 2+ Gigabit Ethernet Switches

Software Release Notes

Please read this document before you begin to use the management software.

Supported Platforms

The AT-S63 Version 2.0.0 management software is supported on the following AT-9400 Series Layer 2+ Gigabit Ethernet switches:

AC Models:

- ☐ AT-9408LC/SP
- ☐ AT-9424T/GB
- ☐ AT-9424T/SP
- ☐ AT-9424Ts
- ☐ AT-9424Ts/XP
- ☐ AT-9448Ts
- ☐ AT-9448T/SP
- ☐ AT-9448Ts/XP

DC Models:

- ☐ AT-9424T/GB-80
- ☐ AT-9424T/SP-80

This release supports the following redundant power supply:

- ☐ AT-RPS3204

(The redundant power supply is only supported on AC models.)

For a list of supported GBIC, SFP, and XFP modules, contact your Allied Telesyn sales representative.

Product Documentation

For hardware installation instructions, refer to the following guide:

- ☐ *AT-9400 Series Layer 2+ Gigabit Ethernet Switches Installation Guide* (PN 613-000357-00)

For management instructions, refer to the following guides:

- ☐ *AT-S63 Management Software Menus Interface User's Guide* (PN 613-50570-00)
- ☐ *AT-S63 Management Software Web Browser Interface User's Guide* (PN 613-50592-00)
- ☐ *AT-S63 Management Software Command Line Interface User's Guide* (PN 613-50571-00)

All documents are available from the Allied Telesyn web site at **www.alliedtelesyn.com**.

Caution:

The software described in the documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesyn sales representative for current information on this product’s export status.

Note:

Prior to version 2.0.0, the Public Key Infrastructure (PKI), Secure Sockets Layer (SSL), and Secure Shell (SSH) encryption features had to be ordered separately. These features are now included as standard components of the AT-S63 management software.

What’s New in Version 2.0.0

Features

- ❑ Internet Protocol Version 4 (IPv4) packet routing. The AT-9400 Series switch now features IPv4 packet routing with routing interfaces, static routes, and the Routing Information Protocol versions 1 and 2. For background information, refer to Chapter 32, “Internet Protocol Version 4 Packet Routing,” in the latest version of the *AT-S63 Management Software Command Line Interface User’s Guide*.
- ❑ Secure Shell (SSH) protocol server. The security of the SSH server on the switch has been enhanced to prevent unauthorized management access to the switch. The AT-S63 management software now disables the SSH server, logs an event in the event logs with the client’s IP address, and sends an SNMP trap if it detects fifty consecutive failed login attempts from an SSH client.
- ❑ Class of Service and Queue 7. The range of the maximum number of transmitted packets for the CoS weighted round robin scheduling method has been changed for Queue 7 (Q7). The range was 1 to 15; the new range is 0 (zero) to 15. Setting Q7 to 0 gives its packets priority over packets in the other queues. No packets are transmitted from the lower priority queues so long as there are packets in Q7. (3803)
- ❑ Temperature threshold alert. The temperature threshold alert feature now has two levels. An ambient temperature of 55° to 60° Celsius for ten minutes activates the first level. The switch sends a SNMP trap and enters a warning event message in the event logs. The second level, activated if the ambient temperature exceeds 60° Celsius for five minutes, sends another SNMP trap, logs an error event message, and activates the Fault LED on the front panel.

Known Issues

- ❑ QoS Policies and Static Multicast Addresses. The behavior of a QoS policy may be unpredictable if a policy's egress port has one or more static multicast addresses. (3196)
- ❑ Remote management session through an 802.1x authenticator port. It may not be possible to ping or remotely manage a switch through an authenticator port set to the 802.1x authentication method and the Multiple Mode. (3451)

Resolved Issues

- ❑ MSTP and LACP. The switch did not forward unicast traffic over an LACP trunk while concurrently running the Multiple Spanning Tree Protocol. This issue has been resolved. (3336)
- ❑ MSTP and SNMP management. Selecting MSTP as the active spanning tree on the switch through SNMP management disabled spanning tree. This issue has been resolved. If spanning tree is enabled prior to the selection of MSTP as the active spanning tree, it remains enabled after MSTP is selected. (3359)
- ❑ Power Supply Status. The status of the main power supply in the AT-9424T/GB and AT-9424Ti/SP switches was erroneously displayed as OFF in the System Hardware Status window in the menus interface and by the SHOW SYSTEM command. The status of the main power supply is now displayed correctly. (3347)
- ❑ Management ACL. You could not modify entries in the Management ACL from the web browser interface. The web browser interface now supports modifying Management ACL entries. (3455)
- ❑ Teardrop DoS defense mechanism. The switch did not display a notification message on the console or send an SNMP trap when it detected or mirrored packets from a possible Teardrop attack. This issue has been resolved. (3456)
- ❑ SFP modules. If you disabled Auto-Negotiation on twisted pair port 23R or 24R or an SFP module in an AT-9424T/SP switch and manually set the speed, the switch displayed an error message if you attempted to change the speed again after the port changed status (i.e., an SFP is removed and the corresponding port 23R or 24R becomes active). This issue has been resolved. (3482)
- ❑ Tagged VLANs and Static Port Trunks. You could not create a static port trunk if the switch had a tagged VLAN. This issue has been resolved. (3589)
- ❑ Egress traffic mirroring across chipsets. The switch did not support egress traffic mirroring across chipsets. This issue has been resolved. (3590)
- ❑ Maximum multicast groups in the web interface. The IGMP Configuration page in the web browser interface had the wrong range for the maximum number of multicast groups. The web page now displays the correct range of 1 to 256. (3591)
- ❑ Save Config button. The web browser interface did not display the Save Config button after a change was made to a RADIUS or TACACS+ parameter. The web browser interface now displays the button. (3246)
- ❑ SHOW CONFIG DYN=QOS command. The SHOW CONFIG DYN=QOS command displayed the weights of the egress queues incorrectly when the QoS scheduling method was weighted round robin and the weight values were consecutive (e.g., 1, 2, 3, etc.). The command displayed the values as a range rather than as individual values. The command now displays the weights of the egress queues as individual values. (3460)

- ❑ MSTP warning message. The command line interface did not display a warning message that changing the MSTP force version from MSTP to STP-compatible deletes all multiple spanning tree instances. The management software now displays a warning message. (3465)
- ❑ SFP speed and duplex mode prompt. The erroneous prompt “10/100/1000Base-T” was displayed alongside the speed and duplex mode settings on an SFP port if you disabled Auto-Negotiation and set the speed manually using the Port Configuration menu in the menu interface. The issue has been resolved. (3481)
- ❑ SET MSTP PORT command. The command line interface did not check for extraneous characters following the AUTO option of the INTPORTCOST and EXTPORTCOST parameters. The issue has been resolved. (3550)
- ❑ Telnet management session. Repeatedly logging in from a Telnet management session and displaying system files caused the management software to stop saving configuration changes to the active boot configuration file and displaying the system files. This issue has been resolved. (3685)
- ❑ atiStkSwSysTrapRecv1-4 MIB object. This MIB object, used to display the IP addresses of the SNMP trap receivers, was nonfunctional. This object is now obsolete. (3260)
- ❑ AT-9448Ts/XP and compact flash. File operations (e.g., copy, delete, etc.) to or from a compact flash card on the AT-9448Ts/XP switch caused the switch management to lockup. This issue has been resolved.

Operational Notes

- ❑ Multiple VLAN modes and IPv4 packet routing. The 802.1Q-compliant and non-802.1Q-compliant multiple VLAN modes do not support IPv4 packet routing. You cannot configure routing interfaces when the switch is running in either of these VLAN modes, and all existing routing interfaces, with the exception of the local interface, are deleted when the VLAN modes are activated. To assign an IP address to a switch for these VLAN modes, you must create one routing interface and designate it as the local interface while the switch is running in the user-configured VLAN mode, and afterwards change the switch's VLAN mode to 802.1Q-compliant and non-802.1Q-compliant. The local interface is automatically moved to the VLAN on port 1 of the switch. (3806)
- ❑ Switch to switch upload of a configuration file. The *AT-S63 Management Software User Guides* state that the configuration file on a master switch retains its routing interface commands when uploaded to a slave switch. This is incorrect when the file is the master switch's active configuration file. All routing interface commands are removed from the master switch's active configuration file when it is uploaded to a slave switch to prevent an IP address conflict on the units. However, uploading any other configuration file on a master switch does not remove the routing interface definitions. (4272)
- ❑ RIP and the spanning tree protocol. The switch, when running both RIP and a spanning tree protocol (STP, RSTP, or MSTP), will not immediately update the ARP table in all circumstances. This can result in a loss of some IP packets. The issue occurs when spanning tree activates a secondary port after the loss of a link on a primary port, and the link on the primary port is later reestablished. When the primary port loses its link, the switch correctly updates the ARP table by deleting all entries learned on the primary port so that it can relearn the ARP entries on the secondary port. However, if the link on the primary port is reestablished and the secondary port is returned to the standby mode, the ARP table is not updated since the link status on the secondary port has not changed, though the port is now in the blocking state. Rather, the old entries remain in the table until they are timed out according to the ARP timeout value. Any IP packets routed using the obsolete ARP entries are discarded. This issue applies to both RIP versions 1 and 2. This issue does not apply to Layer 2 switching. (4168)
- ❑ Telnet management session. Changing the VLAN mode of a switch (e.g., from the user-configured VLAN mode to a multiple VLAN mode) from a remote Telnet management session may end your management session. To continue managing the switch, you must reestablish the management session (3806)
- ❑ SNMPv3 management. The enhanced stacking feature is not supported from SNMPv3. (4065)
- ❑ AtiStkSwVlanConfigEntry MIB table. The response time of the management firmware on the switch will slow if you open more than one instance of the AtiStkSwVlanConfigEntry MIB table at a time. (2231)
- ❑ Compact flash card. Removing a compact flash card from the switch while the management software is writing a file to it may cause the switch to stop responding to management commands and forwarding network packets. To avoid this issue, never remove a compact flash card from the switch while the Fault LED on the front panel is on. Wait for the Fault LED to turn off before removing the card.(4253)

- ❑ LACP priority value and the event log. A change to a switch's LACP priority value is registered in the event log with a message that reflects the current status of LACP, rather than the change to the priority value. The log message is either "lACP:enabled" or "lACP:disabled." (3345)
- ❑ MAC address-based VLANs and static trunks. The documentation states that the ports of a MAC address-based VLAN form a community and that the assignment of a MAC address to one port in a VLAN is equivalent to assigning it to all ports. This is true except in the case where the ports of a MAC address-based VLAN encompass a static port trunk, in which case the same MAC addresses must be assigned to all the ports of the trunk. (3249)
- ❑ File upload or download. The switch's response to management instructions may be delayed while it uploads or downloads a file to the file system.
- ❑ Flow control and back pressure. Flow control and back pressure are operational *among* devices connected to ports 1 through 12 or ports 13 through 24 on the AT-9424T/GB and AT-9424T/SP switches. But flow control and back pressure are not operational *between* devices connected to ports 1 through 12 and 13 through 24. (1321, 1322)
- ❑ Reserved multicast traffic and port mirroring. The destination port of a port mirror may transmit duplicates of some reserved multicast traffic, such as STP BPDUs and other control packets. The duplication results from the destination mirror port transmitting both the reserved multicast traffic it receives from flooded multicast traffic and the same multicast traffic from the mirrored ports. (3055)
- ❑ Fiber optic port configuration display. The Auto-Negotiation, speed, and duplex mode settings in the menus interface for ports 23 and 24 on an AT-9424T/GB or AT-9424T/SP switch always reflect the settings of the corresponding twisted pair ports 23R and 24R. They do not reflect the current settings of an active GBIC or SFP fiber optic port. (3047)
- ❑ GVRP compatibility. There may be some compatibility issues with GVRP and other switches. To work around this situation, change the Join and Leave time from the defaults to: Join Timer = 60 and Leave Timer = 120.
- ❑ Port configuration. The speed, duplex mode, and MDI/MDIX settings of a 10/100/1000Base-T twisted pair port are changed as a unit when configuring multiple ports simultaneously. The settings of the lowest numbered port being configured are automatically copied to the other ports. For example, if you configure ports 1 to 4 simultaneously and change the MDI/MDIX setting, the speed and duplex mode settings of port 1, along with the new MDI/MDIX setting, are copied to ports 2 to 4. (1262)
- ❑ Static and LACP port trunks and load distribution methods. The following load distribution methods for static and LACP port trunks are nonfunctional: source IP address, destination IP address, and source/destination IP addresses. The switch uses source MAC address, destination MAC address, or source/destination MAC addresses, respectively, if one of the nonfunctional load distribution methods is selected.
- ❑ Jumbo frames. Frame loss may occur when jumbo frames are being transferred on more than two ports. (1412, 2783, 2792)
- ❑ Xmodem downloads. The switch does not respond to echo requests or send or respond to STP BPDU packets during an Xmodem download of system software. Also, echo request responses are slowed when there is a TFTP transfer in progress and the echo requests are received within the same port group as the TFTP server. (1663, 1582)

- ❑ SFP and GBIC ports. The switch considers the fiber optic port on an optional SFP or GBIC module in the AT-9424T/GB and AT-9424T/SP switches as active if it is receiving a signal, even if the port has not established a valid link with the remote node. If an optional fiber optic port loses or is unable to establish a link but is receiving a signal, it remains as the active port and the switch does not activate the corresponding twisted pair port 23R or 24R. (2850)
- ❑ Web browser interface. The web browser interface works best with Microsoft Internet Explorer version 6.0 and above. Results using other versions or other web browser applications may vary.
- ❑ Configuration files. Do not use Microsoft's NotePad to edit or view a configuration file. Some versions of NotePad may add formatting codes to the file. Use WordPad instead or some other text editor that will not add formatting codes to the file. When saving the file, do not change the ".cfg" extension in the filename and be sure to save the file without formatting codes.
- ❑ Enhanced stacking. The IP address 172.16.16.16 is reserved for the enhanced stacking feature. Do not assign this address to any device in the same subnet as an enhanced stack.
- ❑ Login password. The maximum length of a login password is 16 alphanumeric characters for manager accounts created through the RADIUS and TACACS+ authentication protocols and supplicant accounts for 802.1x port-based network access control. Passwords that exceed this limit will not work.
- ❑ TACACS+. The TACACS+ client software on the switch supports Password Protection Protocol (PAP), but not Challenge Handshake Authentication Protocol (CHAP) or AppleTalk Remote Access Protocol (ARAP). (1078)
- ❑ Port settings. A port, when removed from a port trunk, retains its settings as a member of the trunk. The parameter settings (e.g., speed and duplex mode) are not returned to the default values. (2144)
- ❑ MAC addresses. You must move the cursor manually from field to field when entering an IP or MAC address in the web browser interface. The cursor does not move automatically as you enter the parts of an address. (1699, 2123)
- ❑ SNTP. The SNTP client software on the switch sends a Transmit Time Stamp with a value NULL when synchronizing with a Network Time Protocol server. This does not affect the operation of the SNTP client software. (1676)
- ❑ IGMP. The switch, when configured for IGMP, will not register tagged IGMP queries in the IGMP routers list if ingress filtering is disabled. (1493)
- ❑ SFP modules and the AT-9408LC/SP switch. Disconnect the fiber optic cable from an SFP module in an AT-9408LC/SP switch before removing the module. The L/A LED for the slot may remain on if you remove an SFP module while it has a link to an end node. This problem does not affect the operation of the switch or the SFP slot. The L/A LED goes off the next time you install an SFP module in the slot.

Features History

Version 1.3.0 of the AT-S63 and AT-S63 NE management software introduced the following new features:

- ❑ Added the following new features to 802.1x port-based network access control:
 - Guest VLANs
 - VLAN Assignment and Secure VLAN features for supporting dynamic VLAN assignments with supplicant accounts.
 - MAC address-based authentication as an alternative to 802.1x username and password authentication.
- ❑ Simplified the menu interface for managing the access control entries in the Management ACL.

Version 1.2.0 introduced the following new features:

- ❑ MLD snooping for MLDv1 and MLDv2.
- ❑ 802.1x port-based network access control has been enhanced to support up to 20 supplicants simultaneously on an authenticator port.
- ❑ Quality of Service has been enhanced with the following new actions:
 - Set Type of Service (ToS)
 - Move Type of Service to 802.1p Priority
 - Move 802.1p Priority to Type of Service
 - Send to Mirror Port
- ❑ The command line interface has been enhanced with new command parameters for displaying and deleting specific types of MAC addresses from the MAC address table.

Version 1.1.0 introduced the following new features:

- ❑ LACP (802.3ad)
- ❑ Policy-based QoS (Classifiers, Flow Groups, Traffic Classes, and Policies)
- ❑ Flash memory operations
- ❑ Access Control Lists (ACLs)
- ❑ Syslog support
- ❑ Password reset
- ❑ Redundant power supply information
- ❑ IGMP v3 Snooping
- ❑ New web browser interface procedures

Version 1.0.0 supported the following features:

- ❑ Auto-Negotiation (IEEE 803.3u-compliant) for speed and duplex mode
- ❑ Auto and manual MDI/MDI-X
- ❑ Flow control (IEEE 802.3x and 802.3z-compliant)
- ❑ Head of line blocking prevention
- ❑ Unicast, multicast, and broadcast rate control
- ❑ Port mirroring

- ☐ Port trunking (IEEE 802.3ad) (static link aggregation, non LACP)
- ☐ Port security
- ☐ Port statistics (RMON)
- ☐ 1000 static MAC addresses, 16K dynamic MAC addresses, 256 static multicast addresses, 255 dynamic MAC addresses (snooping)
- ☐ Spanning Tree Protocol (IEEE 802.1D)
- ☐ Rapid Spanning Tree Protocol (IEEE 802.1w)
- ☐ Multiple Spanning Tree Protocol (IEEE 802.1s)
- ☐ Virtual LANs (IEEE 802.1Q)
- ☐ Protected ports VLANs
- ☐ Ingress filtering
- ☐ GARP VLAN Registration Protocol (GVRP)-based dynamic VLANs
- ☐ Secure Sockets Layer (SSL) Protocol (not included in AT-S63 NE)
- ☐ Secure Shell (SSH) Protocol (not included in AT-S63 NE)
- ☐ Public Key Infrastructure (PKI) Certificates (not included in AT-S63 NE)
- ☐ Static and dynamic system time (SNTP client)
- ☐ Management VLAN
- ☐ Multiple VLAN modes
- ☐ Event log
- ☐ Enhanced stacking (for management)
- ☐ IGMP Snooping (RFC 2236)
- ☐ Class of Service (IEEE 802.1p-compliant)
- ☐ Queuing - map 802.1p to CoS queue to prioritize traffic at egress
- ☐ Strict priority and weighted round robin priority scheduling
- ☐ RRP Snooping
- ☐ File system
- ☐ SNMPv1, SNMPv2c and SNMPv3 management
- ☐ CLI-based configuration file
- ☐ Denial of Service detection
- ☐ 802.1x Port-based Network Access Control
- ☐ RADIUS accounting
- ☐ Menus, CLI, web, and SNMP interfaces
- ☐ Password protected management access
- ☐ Management access control list
- ☐ Local authentication
- ☐ RADIUS and TACACS+ authentication protocols
- ☐ Xmodem and TFTP downloads and uploads, HTTP and enhanced stacking
- ☐ Static IP configuration

- ❑ BOOTP and DHCP
- ❑ Fan and temperature information
- ❑ CPU, Flash, and RAM information
- ❑ Power supply, redundant power supply, and transceiver information

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base at **www.alliedtelesyn.com/kb**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesyn without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn's Technical Support group through our web site: **www.alliedtelesyn.com**.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information on our web site: www.alliedtelesyn.com. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Obtaining Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- ☐ Allied Telesyn web site: **www.alliedtelesyn.com**
- ☐ Allied Telesyn FTP server: **<ftp://ftp.alliedtelesyn.com>**

To download new software from the Allied Telesyn FTP server from your workstation's command prompt, you need FTP client software. You are asked to log in to the server. Enter "anonymous" as the user name and your email address for the password.